~~1/2~~

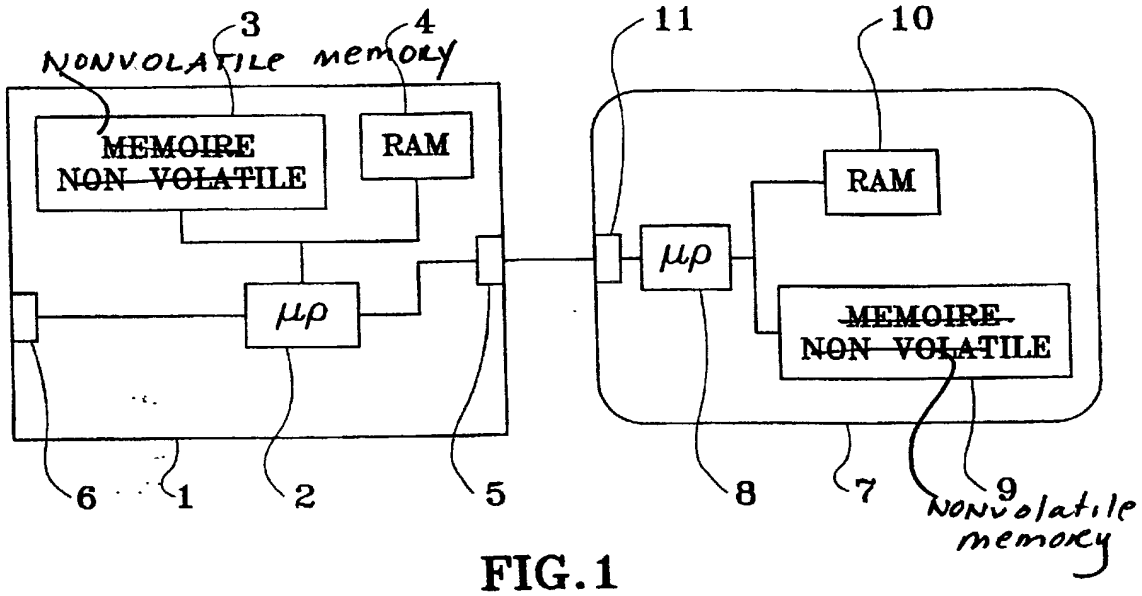
3
4
NONVOLATILE memory
MEMOIRE NON VOLATILE
RAM
µp
11
10
RAM
µp
MEMOIRE NON VOLATILE
6
1
2
5
8
7
9
NONvolatile memory

FIG.1

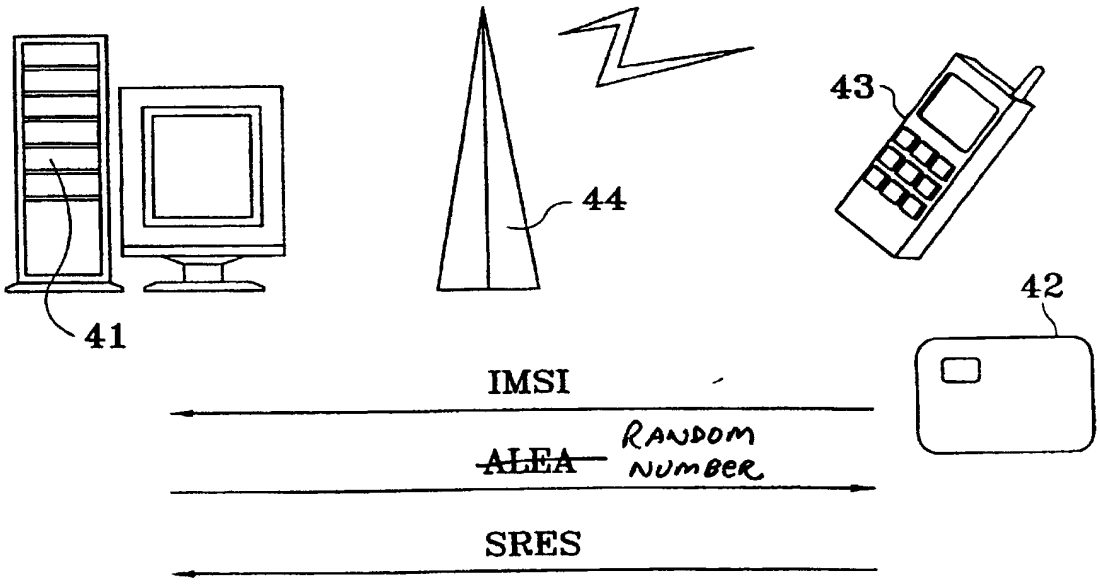
43
44
42
41
IMSI
~~ALEA~~ RANDOM NUMBER
SRES

FIG.4

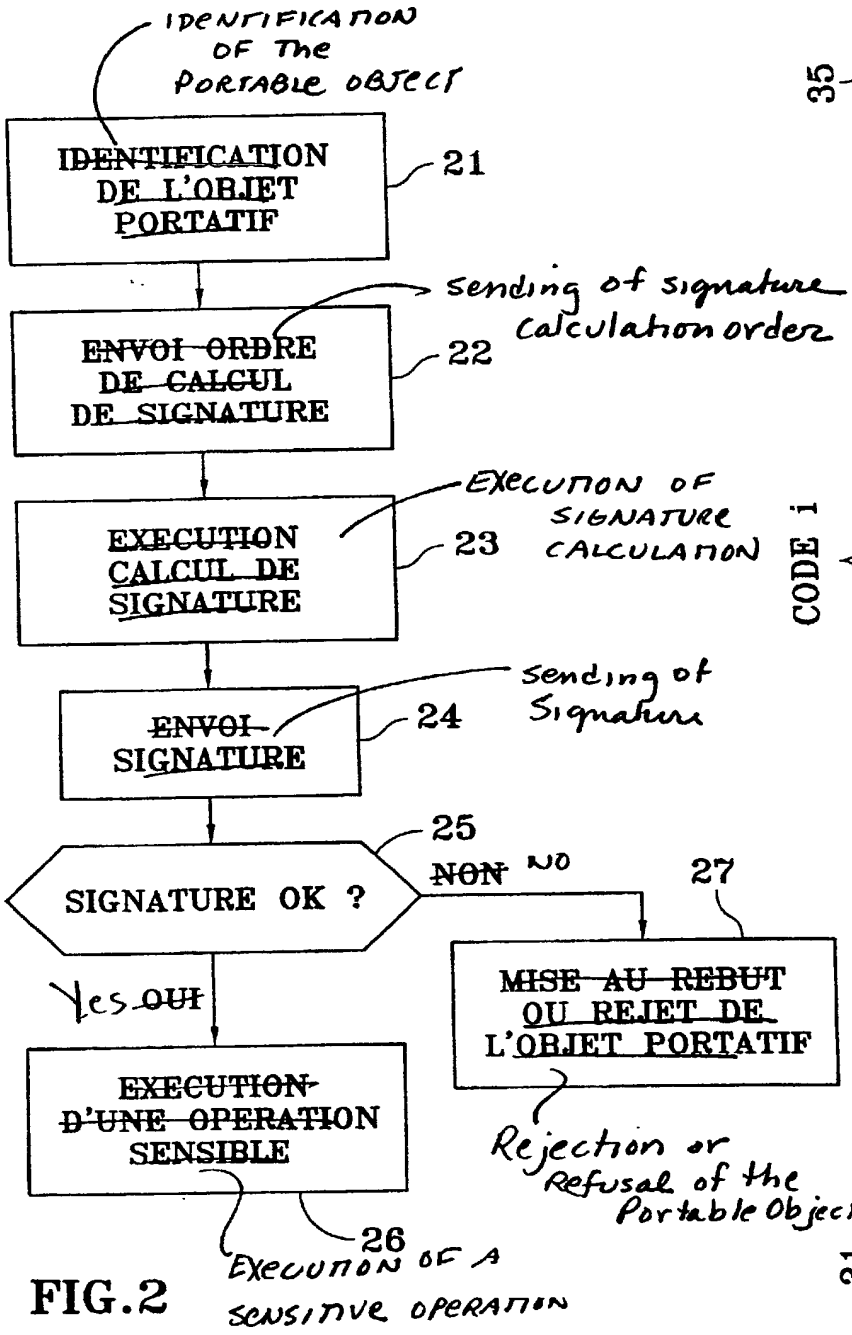
IDENTIFICATION OF THE PORTABLE OBJECT
IDENTIFICATION DE L'OBJET PORTATIF
21
sending of signature calculation order
ENVOI ORDRE DE CALCUL DE SIGNATURE
22
EXECUTION CALCUL DE SIGNATURE
23
EXECUTION OF SIGNATURE CALCULATION
ENVOI SIGNATURE
24
sending of Signature
25
SIGNATURE OK ?
NON NO
27
Yes OUI
MISE AU REBUT OU REJET DE L'OBJET PORTATIF
EXECUTION D'UNE OPERATION SENSIBLE
Rejection or Refusal of the Portable Object
26
EXECUTION OF A SENSITIVE OPERATION

FIG.2

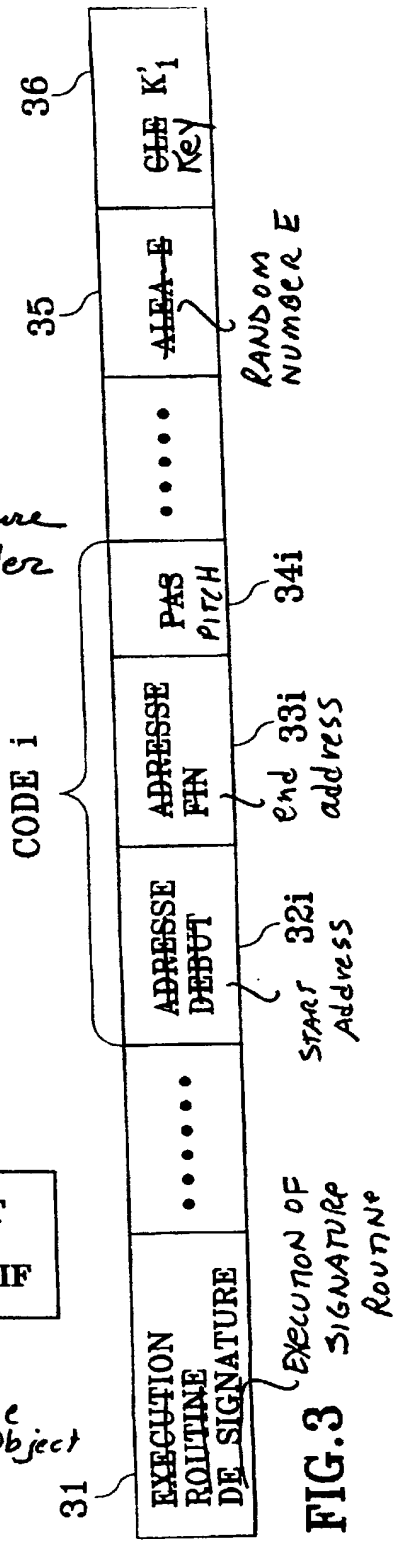
36
CLE K'1
Key
35
ALEA E
RANDOM NUMBER E
.....
PAS
PITCH
34i
ADRESSE FIN
33i
end address
ADRESSE DEBUT
32i
start Address
CODE i
.....
EXECUTION ROUTINE DE SIGNATURE
31
EXECUTION OF SIGNATURE ROUTINE

FIG.3